DEPARTMENT OF THE NAVY
OFFICE OF THE COMPTROLLER
WASHINGTON, D.C. 20350-1100

IN REPLY REFER TO

NAVCOMPTINST 7270.2
NAFC-5424
24 DEC 1990

NAVCOMPT INSTRUCTION 7270.2

From: Comptroller of the Navy

Subj: ELECTRONIC TRANSMISSION OF FINANCIAL INFORMATION

Ref: (a) GAO Policy and Procedures Manual for Guidance of Federal Agencies - Fiscal Procedures, Title 7 (NOTAL)
(b) SECNAVINST 5239.2 of 15 Nov 89
(c) OPNAVINST 5239.1A of 1 Apr 85
(d) SECNAVINST 5211.5C of 11 July 86

Encl: (1) Electronic Transmission of Financial Information

1. Purpose. To establish policy and provide guidance to the Department of the Navy regarding electronic transmission of financial information. Financial information includes the telecommunication of: (1) funding documents, (2) receipt and acceptance certification, (3) invoices, (4) payment certification, (5) funds transfer, and (6) individual financial information included under the Privacy Act of 1974 (P.L. 93-597).

2. Cancellation. NAVCOMPTINST 7270.1.

3. Scope. This instruction applies to activities responsible for transmitting financial information within the Department of the Navy. These procedures do not apply to transactions occurring outside of Navy, e.g., Defense Contract Management Districts (DCMD), unless specific agreements have been established.

4. Background. There is an opportunity to process data faster and provide more timely information for management. Electronic techniques and Automated Information Systems (AISs) are being used to generate, process, transmit and store financial information. Electronic transmission of financial information will help deal effectively with the high-volume of financial transactions, geographic dispersion of activities, and the requirements of prompt payment in today's financial environment. In this environment, it is impractical for an accountable official to examine personally each transaction for which he or she accepts responsibility. Consequently, in fulfilling his or her responsibilities, accountable officials must be able to rely on systems, controls and personnel that process transactions.

5. Policy

a. Acceptance of electronically transmitted information is dependent on the accountable officials being able to rely on key processes and controls in the AISs providing electronic input to them. This instruction incorporates the controls specified in references (a) through (d).

b. Financial information will be transmitted electronically when it is determined to be a cost effective method, considered desirable to meet time requirements, acceptable to the receiving activity/functional area, and meets the applicable security requirements. Various source documents can be transmitted, and the exchange of information can be internal and/or external to the activity or functional area. As a general policy, activities should endeavor to establish automated processing techniques and controls wherever they are feasible. They should not, however, view the use of these procedures as a relaxation of examination and approval requirements.

c. Electronic transmission of financial information requires strong management control. System controls must be documented, tested and certified that they provide reasonable assurance that electronically transmitted information is complete, correct, authorized, and secure. Implementation of electronic technology requires that the financial processing system be carefully structured and monitored to ensure that audit trails are maintained and that officials who are responsible for authorizing, certifying and disbursing are in possession of the information needed to carry out their responsibilities.

6. Action

a. Commands and activities who implement electronic financial data transmission capabilities, will certify in writing to the activity receiving the transmitted information that all the requirements in enclosure (1) have been met. Enclosure (1) provides the minimum controls that must be implemented. Appendices A through E to enclosure (1) are applicable to specific areas of responsibility and must be followed in addition to this general policy. The controls prescribed in this instruction are designed to provide reasonable assurance that deliberate or inadvertent manipulation, disclosure, modification or loss of data during transmission will be detected. If functions are performed within the same activity the same controls apply. Agreements between activities/parties should be in writing when information is to be exchanged electronically.

b. Activities with financial AISs currently using electronic transmission capabilities will review operations to ensure compliance with this instruction. An activity with an operating system which employs electronic procedures significantly different from this instruction and who projects lengthy delays for corrective action, should advise the Navy Accounting and Finance Center who will assist in determining adequacy of the system for electronic processing.

c. Design Agents will:

(1) Incorporate required security measures throughout the system and application software architecture.

(2) Ensure consistency and compatibility of interfaces among the various accounting, disbursing, personnel, supply, travel and contract administration systems.

(3) Provide the capability to identify and suspend suspected duplicate information.

(4) Provide full audit trail capability to maintain accountability and control within the system.

J. T. KAVANAUGH
By direction

Distribution:
SNDL Part 2

Stocked:
CO, NAVPUBFORMCEN
5801 Tabor Avenue
Philadelphia, PA 19120-5099 (200 copies)

ELECTRONIC TRANSMISSION OF FINANCIAL INFORMATION

1. General requirements that must be met:

a. Internal controls must be identified, documented, instituted, and tested for both on-line and batch processing of electronically transmitted information.

b. Managers will receive periodically, a summary of all transactions or events for each password user.

c. Civilian and military managers who are responsible for internal controls must be identified at each activity.

d. Duties and functions must be separated to minimize opportunities for carrying out unauthorized, fraudulent or otherwise irregular acts.

e. The responsibilities of each individual within the processing chain must be defined and documented to ensure integrity of the system. When information is transmitted outside an activity, a memorandum of understanding must be signed by applicable authorities and include security controls.

f. The performance appraisal systems for managers must reflect management (internal) control responsibilities.

g. Documentation (e.g. hard copy, microfilm, microfiche, or tape) must be retained at the point of original action for audit purposes. Controls required over support documentation do not change with this instruction, only the method by which it is obtained and maintained.

h. Backup should be made of electronically transmitted financial information as a preventive measure to minimize the effects of a loss of information.

i. Managers must periodically test the system and review testing by others for compliance with the original design documentation and later changes. Tests should confirm key processing procedures and controls are working and reliable. Management testing methods may include management control reviews, system manager/user reviews or ad hoc studies. Testing by others may take the form of Consolidated System Evaluation (CSE), inspections, audits, or management studies. System managers must ensure that changes or enhancements made have not negated or downgraded the system's overall level of internal controls.

2. ADP Security requirements that must be met:

a. General

(1) Security requirements for AISs (e.g. mainframe, mini and personal computers, terminals, etc.) are identified among several sources within Department of Defense (DOD), Department of the Navy (DON), and other Federal agencies. Compliance with all of the minimum mandatory security requirements of references (b) and (c) and other related instructions is required. Compliance with reference (d) and the Privacy Act of 1974 (includes personal financial information within AISs) is also required.

(2) The following minimum password management guidelines must be followed on all AIS systems processing or containing financial information and/or Privacy Act information.

(a) A password is a character string used to authenticate a user identity and the knowledge of which is considered proof of authorization to use the capabilities associated with that user. Accordingly, passwords:

1. Must be assigned to all personnel requiring access.

2. Must be encrypted.

3. Must be changed at least every six months.

4. Must be invalidated when the assigned user no longer has authority for which the password was issued, and when information becomes available suggesting that the password has been compromised.

5. Must be authorized for use at specific terminals only. If it becomes necessary to use an alternate terminal because of equipment malfunctions or other similar situations, the data base manager and the ADP security officer shall have the authority to permit temporary use of an alternate terminal. Lockout controls shall be used to prevent unauthorized use.

6. Must be issued to one individual only. Sharing passwords by two or more individuals shall be prohibited.

7. Shall be issued to, and withdrawn from, designated individuals by ADP security officers or data base

administrators only upon receipt of an original written request signed and dated by an official having authority to issue such requests. Such authorizing officials shall not be permitted to redelegate this authority.

(b) ADP security officers or data base administrators shall retain indefinitely the written requests for password issuances. Indefinitely means as long as the individual to whom the password was issued is authorized to use the password or three years after the password is withdrawn from use upon a request for withdrawal.

(c) Before renewing password authority, ADP security officers or data base administrators shall determine that the individual to whom the password was originally issued continues to have a valid need for the password. This determination shall be made by requesting the authorizing official to certify that each such individual continues to perform the duties for which the password was originally issued. Such certification shall be in writing and signed by the authorizing official.

(d) When an authorizing official is reassigned, the successor authorizing official shall provide the ADP security officers or data base administrators a signed and dated listing of those individuals for whom continued use of passwords is authorized.

(e) When ADP security officers or data base administrators are reassigned or otherwise relieved of their duties, passwords shall be changed.

(f) The number of persons having authentic passwords shall be held to the minimum necessary for efficient operations.

(3) Password users:

(a) Shall not disclose, or otherwise permit others to use, assigned passwords.

(b) Shall immediately notify the ADP security officer or data base administrator when they have reason to believe that assigned passwords have been compromised. This applies to their own password as well as any other authorized passwords.

(c) Shall receive periodically, but at least monthly, a summary of all transactions or events for which they used the password. This listing may be displayed on the terminal monitor or be in hard copy form. The purpose of the listing is to provide users the capability of determining that no unauthorized

password use had occurred during the period covered by the list. The listing shall show, among other data, the date and time the authentication password was used, the identification number of terminal used, the type of transaction involved (obligation, receiving order, disbursement, etc.), and the dollar value of the transaction, if applicable. The recipient shall notify designated higher officials of any suspected misuse in writing.

b. Telecommunication

(1) During telecommunication of designated financial information, Public Key Cryptography (PKC) and electronic signatures must be used. Electronic signature is a means within an AIS whereby a unique code is affixed to a document or file which allows only that activity's designated authority to certify a transmission and be authenticated by only the responsible person on the receiving end. Public keys and electronic signatures must meet the following requirements:

(a) Must use PKC and/or Data Encryption Standard (DES) for authentication and protection of telecommunicated, financial information.

(b) Public keys must be certified by the originator prior to their exchange and also certified by the recipient immediately upon its receipt.

(c) Public keys may be distributed by either electronic or manual means between certifying and receiving officials.

(d) Private keys must be protected from unauthorized access/disclosure and not distributed to anyone.

(e) Public and private keys must be changed once a year at a minimum.

(f) Electronic signatures must be originated by only the designated certifying official.

(g) Electronic signatures must be authenticated by only the designated receiving official.

(h) Electronic signatures must include the certifying official's approval or disapproval, name, and title.

(i) Electronic signatures may be used in instances where an authorized signature must be present on a hardcopy document.

(j) During telecommunication of Privacy Act information, both PKC and DES encryption must be used.

(k) Any deviations from the above public key and electronic signature requirements for financial and Privacy Act telecommunications must receive prior approval from the NAVCOMPT/NAFC ADP Security Officer before implementation.

3. Appendices A through E are applicable to specific areas of responsibility and must be followed in addition to this general policy.

ELECTRONIC FUNDING DOCUMENTS

1. Purpose. To establish policy and set forth methodology to use electronic means of transmitting funding documents. This category of documents includes any division of budget authority and obligating documents.

2. Scope. This applies to activities who have the capability to electronically transmit and receive funding documents.

3. Specific Requirements

a. When multiple levels of approval are required, systems shall be designed so that approvals occur in ascending order and that no level can be bypassed, except by only the next higher level.

b. Disapproval by any level shall stop the transaction processing. Such disapprovals shall include a justification entered into a designated area on the terminal monitor. Disapproved transactions shall be returned to the previous approval level unless the disapproval occurred at the first level.

c. When a source document is available, it shall be annotated to show, among other things, that the transaction was entered into the system, the date and time of entry, and that electronic signature authentication was used. This does not mean that each individual using an authentication password must annotate the document. It only means that the document must show that all approvals were performed electronically. One way of achieving this would be affixing to the source documents the statement "Electronic signature approvals used."

d. When electronic signatures are used in the process of generating a final document such as a travel order, a requisition, or a purchase order, the hard copy document shall be produced only after the final approval is received. The official signing the document must ensure the electronic equivalent of a signature is contained on electronic or terminal accessed document.

e. When the transaction results in an obligating document, the fund availability authentication shall be a required step of approval in the electronic authentication process.

f. When a transaction requires both authentication and approval or acceptance signatures, i.e., project order, work request, a method of authenticating each approval must be established and accountability for source documentation determined.

ELECTRONIC RECEIPT AND ACCEPTANCE CERTIFICATION

1. Purpose. To establish policy and set forth methodology to implement the use of electronic signature to evidence receipt and acceptance for goods and services.

2. Scope. This applies to all activities responsible for: (1) certifying the physical receipt and acceptance of materials and services for the Department of the Navy; and (2) bill paying, where electronic systems are available to support the process. These procedures do not apply to contracts administered by or paid by the Defense Logistics Agency activities, or other DOD services since cross disbursing agreements direct support requirements between services.

3. Specific Requirements

a. Receiving and accepting activities will:

(1) Provide written certification to the bill paying activity that the electronic receipt and acceptance certification system complies with the requirements established in this instruction;

(2) Use the most expeditious means, e.g. electronic file transfer, mailed tape, etc., to forward certified receipt and acceptance data to the servicing bill paying office in those instances where direct terminal access or electronic interfaces are not available; and

(3) Ensure the electronic equivalent of an authorization and/or acceptance signature is contained on electronic or terminal accessed document;

(4) Retain hard copy or mechanized evidence of receipt and acceptance source documentation at the point of original action.

b. Disbursing Officers (DO) will:

(1) Pay invoices based on electronic receipt authentication and acceptance authentication. All other paying requirements must continue to be met; and

(2) Test, at their discretion, the system to ensure that key processes and controls are in place and operating as designed. Electronic signature will be considered an acceptable signature certification.

However, if testing concludes that the internal controls are inadequate or key processes are not operating as intended, the DO has the right to require submission of source documentation to support disbursements.

ELECTRONIC INVOICE TRANSMISSION REQUIREMENTS

1. Purpose. To establish policy and set forth methodology to implement electronically transmitted vendor invoices. These procedures do not in any way relieve an activity from complying with the procedures provided in the NAVCOMPT Manual. Electronically transmitted invoices shall be treated the same as hard copy invoices.

2. Scope. This applies to electronically transmitted vendor invoices at (1) activities where acceptance and certification of the invoices takes place and (2) bill paying activities, where electronic systems are available to support the process.

3. Specific Requirements

a. A valid electronic invoice must contain the following minimum information:

(1) Contractor name and address
(2) Contractor invoice number
(3) Contractor invoice date
(4) Remittance address
(5) Contract number
(6) Invoice gross amount
(7) Invoice line item description
(8) Invoice line item quantity
(9) Invoice line item amount
(10) Discount terms (if applicable)

b. Invoices transmitted from the Accepting Activity to the Bill Paying Activity. The following additional information must be contained on all electronically transmitted invoices from the acceptance office to the paying office:

(1) Date the goods or services were accepted
(2) Date the goods or services were received
(3) Date the Contractor's invoice was received
(4) Date the Contractor's invoice was sent to the designated paying office
(5) Contract Line Item Number (CLIN) (if applicable)
(6) Contract Sub-Line Item Number (SLIN) (if applicable)
(7) Shipment number (if applicable)
(8) Destination of shipment (if applicable)
(9) Name of acceptance activity

c. Retention of invoices for audit purposes. The bill paying activity will ensure an electronic equivalent of every

invoice transmitted is available for hard copy print out.

d. Return of invoices. Electronically transmitted invoices that need to be returned to the vendor may also be returned electronically. The transmitted invoice must be accompanied by an electronic message reporting the reason for return.

e. Criteria for suspected duplicate payments. Internal controls must be in place to prevent duplicate payments of invoices. The process for checking duplicate payment must be followed per NAVCOMPT Manual paragraph 04080412.

ELECTRONIC PAYMENT CERTIFICATION

1. Purpose. To establish policy and set forth methodology to implement electronic payment voucher certification. This category of documents includes all items required to support a disbursement other than obligating documents, which are discussed under "Funding Documents" (Appendix A).

2. Scope. This applies to vouchers that have met the electronic receipt and certification requirements and have been transmitted to the authorized bill paying/disbursing activity.

3. Definition. Electronic payment certification is an automated process between the disbursing office and the certifying office that verifies the validity of expected payments. Verification is performed from electronically submitted documents and may be done entirely by the system.

4. Specific Requirements

a. Documentation required to support disbursements will be based on evidence of a valid contract, obligation document, receipt and acceptance, and invoice, whether issued by electronic certification techniques or hard copy.

b. When electronic payment certification techniques are used, it is not necessary to physically transfer the hard copy documentation to the paying office for examination.

c. A copy of the certified electronic invoice must be retained. The disbursing activity will ensure an invoice file is developed in the bill paying system which will permit post payment audit and review.

d. In order for the DO to pay invoices, the receiving and accepting activity using electronic certification techniques must assure internal controls are acceptable. The controls must provide for accountability, tracking, an audit trail (e.g., when transmitting electronically the hard copy document must be archived into system) and to protect against unauthorized transmissions and duplicate payments. These controls include:

(1) Providing tracking to invoice file and ensuring an audit trail exists for certified electronic invoices.

(2) Ensuring rejected copies of originating activities invoice are maintained.

(3) Determining that the payment data has not been altered since being transmitted from its point of origin and after transmission to the Federal Reserve Bank (FRB) following message authentication specifications in the American National Standard Financial Institution (ANSI) X9.9 Message Authentication.

e. Disbursing officers shall have the opportunity to test, at their discretion, the suitability of such internal controls and to assure themselves that such internal controls are in place and operating as designed.

f. Proposed disbursement shall be finalized and released for payment by electronic signature capability only when all required electronic certifications have been recorded in the system. These certifications shall include, but are not limited to:

(1) Evidence that a valid contract and/or obligations have been established and recorded in the accounting systems;

(2) Evidence that goods and services have been received; and

(3) Evidence that invoices have been received and matched to the obligating documents and receiving reports.

g. Disbursing officers shall retain the option of having source documents supporting proposed disbursements transmitted to designated sites if they conclude that the internal controls related to the obligation, receipt of goods and services, and processing of invoices are inadequate or are not operating as intended.

h. When the disbursing officer relies on the commanding officer of the sending activity for payment certification, the commanding officer will perform a yearly examination of their system at that activity. The disbursing officer will maintain a file containing the current certifications from each activity providing payment certification.

ELECTRONIC FUNDS TRANSFER (EFT)

1. Purpose. To establish policy and set forth methodology to implement EFT. The following procedures pertain to government payments made for deposit to financial institution (FI) accounts through the Federal Reserve Bank/Automated Clearing House (FRB/ACH) network using the EFT method.

2. Scope. This applies to electronic transmission of data for the purpose of disbursing funds for payment of certified vouchers and/or payment of government benefit salary payments from the authorized bill paying/disbursing activity.

3. Specific Requirements

a. Central Design Agents and data processing centers responsibilities:

(1) Provide systems capability to accommodate EFT payments conforming to the National Automated Clearing House Association (NACHA) and American National Standard Institute, (i.e., ANSI ASC X12) standards and prescribed formats for electronic data interchange;

(2) Ensure data transmitted to the FRB is generated and protected following ANSI X9.9 Financial Institution Message Authentication standards; and

(3) Test software package for systems operability before releasing to payment site for installation.

b. Disbursing activity responsibilities:

(1) Execute MOA with local FRB for EFT transmission;

(2) Successful testing and prenotification with zero dollar amounts through the FRB and FI network is required before disbursing activity is approved to go with live payment operation;

(3) Payment of vendor bills must be transmitted to the FRB at the minimum one business day (24 hours), or as agreed upon between disbursing activity and FRB prior to the settlement/payment due date. This will ensure payment is forwarded to the vendor's financial institution on time. The FRB is responsible for ACH processing to vendor's bank which must meet the Prompt Payment Act requirements; and

(4) After successful EFT transmission of payment is complete the disbursing officer is responsible for preparing the facsimile Debit Voucher (SF 5515) to the FRB for the total number of invoices released. An original will be mailed.